REMARKS

As stated above, the applicant appreciates the examiner's thorough examination of the subject application and requests reexamination and reconsideration of the subject application in view of the preceding amendments and the following remarks.

Concerning Item 3 of the subject action, the Examiner objects to claim 39, asserting that there exists a noun-verb mismatch. Specifically, concerning the phase "is substantially similar to the SA generated", the subject of this phrase is "said SA" and is not "at least one network adaptor". Accordingly, the applicant respectfully asserts that the phrase is proper and, therefore, no amendment is necessary.

Concerning Items 4 & 5 of the subject action, the Examiner rejects claims 25-26, 30-31, 35-36, and 40-41 under 35 USC §112, asserting that the claims fail to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. In response to this rejection, applicant has amended claims 25-26, 30-31, 35-36, and 40-41 to modify "and has computations" to read "and hash computations".

Concerning Items 6-7 of the subject action, the Examiner rejects claims 24-43, under 35 USC §103(a), based on the combination of the teachings of Anand et al (U.S. Patent No.: 6,370,599) and Yoshida (U.S. Patent No.: 5,928,372).

Applicant claims (in currently amended claim 24):

> 24. (Currently Amended) A method, comprising: receiving, by a network adapter, a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA) and provided to said network adapter via a network infrastructure; generating, by said network adapter, a second integrity indicator based on said SA; and verifying, by said network adapter, that said SA within said network adapter is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator.

Applicant claims (in currently amended claim 29):

> 29. (Currently Amended) An apparatus, comprising: a network adapter comprising an integrated circuit, said integrated circuit is capable of receiving a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA) and provided to said network adapter via a network infrastructure, said integrated

circuit being further capable of generating a second integrity indicator based on said SA, said integrated circuit being further capable of verifying that said SA received by said integrated circuit is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator.

Applicant claims (in currently amended claim 34):

34. (Currently Amended) An article comprising: a storage medium storing instructions that when executed by a machine result in the following operations: receiving, by a network adapter, a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA) and provided to said network adapter via a network infrastructure; generating, by said network adapter, a second integrity indicator based on said SA; and verifying, by said network adapter, that said SA within said network adapter is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator.

Applicant claims (in currently amended claim 39):

39. (Previously Presented) A system, comprising: at least one network adapter being capable of being coupled to an information handling apparatus (IHA) via a bus, said network adapter comprising an integrated circuit capable of receiving a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by said IHA and provided to said network adapter via a network infrastructure, said integrated circuit being further capable of generating a second integrity indicator based on said SA, said integrated circuit being further capable of verifying that said SA received by said integrated circuit is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator.

Applicant respectfully asserts that the combination of the teachings of Anand and Yoshida fails to disclose the underlined portions of applicant's claims 24, 29, 34 and 39, namely "said SA and first integrity indicator … … provided to said network adapter via a network infrastructure". Accordingly, applicant respectfully asserts that the combination of the teachings of Anand and Yoshida is not a proper basis for a 35 USC §103(a) rejection, as the combination of the teachings of Anand and Yoshida fails to disclose each and every element of the applicant's claimed invention.

Specifically, the Examiner states that:

> Yoshida teaches data verification in a data transfer system in which a host processor transfers data and a first integrity indicator generated by the host processor to a peripheral device (i.e., the hard disk unit) and the peripheral device generates a second integrity indicator, verifies that the received data is similar to the data sent by the host processor by comparing said first integrity indicator to said second integrity indicator (col. 1, line 60 – col. 2, line 20; figures 20-21 and corresponding text).

Concerning the passage of Yoshida relied upon by the Examiner, the passage discloses:

> A transfer data verification method in the data processing equipped with an external recording unit according to the present invention for accomplishing the object described above is a method of verifying transferred data in a data processor which incorporates a main board having a microprocessor mounted thereto and an external recording unit for storing data, and wherein the data transfer is effected between the main board and the external recording unit through a specific interface, and this method comprises a first stage in which, when the data transfer is effected between the data processor and the external recording unit, a data check code having a one-byte width is calculated on the data processor side by a predetermined calculation formula by regarding this transfer data as serial data; a second stage in which, when the data transfer is effected between the data processor and the external recording unit, a data check code having a one-byte width is calculated on the side of the external recording unit by the same predetermined calculation formula as that of the data processor side on the side of the external recording unit by regarding the transfer data as serial data; a third stage in which, after the data transfer is completely finished, the data check code calculated on the side of the data processor is compared with the data check code calculated on the side of the external recording unit; and a fourth stage in which, when these two data check codes coincide with each other, the data transfer is judged as being effected without error, and when they do not coincide, the data transfer is judged as not being effected normally. *See Yoshida, col. 1, line 60 – col. 2, line 20; emphasis added.*

Yoshida discloses a system that verifies the integrity of data transferred between a "main board" and an "external recording unit". Accordingly, Yoshida fails to teach a system that allows for the verification of data between network devices.

Further, while the Examiner asserts that "Anand and Yoshida are analogous art because they are from a similar problem solving area, which is transferring data from a host processor to a peripheral device", applicant respectfully disagrees with this assertion.

Upon reviewing Yoshida, it is readily apparent that Yoshida concerns data transfers between a computer motherboard and an internal hard disk drive. Accordingly, the data transfer

events that are handled by the Yoshida system are comparatively secure, as the data doesn't leave the sanctity of the computer system. However, the data transfer events that are handled by the applicant's system are substantially more prone to attack / corruption, as the data is provided through a network infrastructure. Accordingly, applicant respectfully asserts that Anand and Yoshida are not analogous art, as the security / corruption risks associated with providing data between a motherboard and a hard disk drive (as disclosed in Yoshida) are quite different than those associated with transferring data between two network devices via a network infrastructure.

Accordingly, the applicant respectfully asserts that the combination of Anand and Yoshida is not a proper basis for a 35 USC §103(a) rejection, as the combination of the references fails to disclose each and every element of the applicant's currently amended claims 24, 29, 34 and 39. Therefore, the applicant respectfully asserts that independent claims 24, 29, 34 and 39 are patentable over the combination of cited references.

As dependent claims 25-28 depend (either directly or indirectly) upon independent claim 24, applicants respectfully assert that claims 25-28 are also patentable over the combination of cited references. Further, as dependent claims 30-33 depend (either directly or indirectly) upon independent claim 29, applicants respectfully assert that claims 30-33 are also patentable over the combination of cited references. Additionally, as dependent claims 35-38 depend (either directly or indirectly) upon independent claim 34, applicants respectfully assert that claims 35-38 are also patentable over the combination of cited references. Finally, as dependent claims 40-43 depend (either directly or indirectly) upon independent claim 39, applicants respectfully assert that claims 40-43 are also patentable over the combination of cited references.

No new matter has been added by these amendments. The applicants respectfully assert that the subject application is now in condition for allowance. The Examiner is invited to telephone Applicant's attorney (603-668-6560) to facilitate prosecution of this application. Please apply any charges or credits to deposit account 50-2121.

Respectfully submitted,

AVRAHAM MUALEM ET AL.

By their Representatives,

Customer Number 32047
Telephone Number 603-668-6560

Date 09 August 2005

By _____
Brian J. Colandreo
Reg. No. 42,427

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 9th day of August, 2005.

Chris Hammond
Name

_____
Signature